

Marktconsultatie MDR/SOC dienstverlening ten behoefte van veiligheidsregio's en het NIPV

Nederlands Instituut Publieke Veiligheid
Kemperbergerweg 783
6816 RW Arnhem
www.nipv.nl
info@nipv.nl
088 - 274 74 00

Colofon

Opdrachtgever:	Nederlands Instituut Publieke Veiligheid
Contactpersoon:	Nanet Kunst
Titel:	Marktconsultatie MDR-dienstverlening ten behoeve van het NIPV en veiligheidsregio's
Datum:	3 maart 2025
Status:	Definitief
Versie:	1

Voorwoord

Het Nederlands Instituut Publieke Veiligheid (NIPV) en verschillende veiligheidsregio's zijn voornemens om Managed Detection & Respons (MDR) dienstverlening aan te besteden. Het NIPV en de veiligheidsregio's (de deelnemers) hebben besloten hiervoor gezamenlijk een marktconsultatie te houden, waarin het NIPV de uitvoering van de marktconsultatie verzorgt en de resultaten zal delen met de veiligheidsregio's. Deze marktconsultatie is bedoeld om de mogelijkheden in de markt te verkennen in aanloop naar de aanbestedingsprocedure.

Aan de hand van de uitkomsten van deze marktconsultatie bepalen het NIPV en veiligheidsregio's of de opdracht in de markt gezet gaat worden en hoe (gezamenlijk, deels gezamenlijk of elke veiligheidsregio en het NIPV individueel). De uitkomsten dienen dan tevens ter bepaling van de aanbestedingsstrategie en wordt eventueel ingezet ter voorbereiding op een aanbesteding of, indien passend, een eventuele percelenindeling en zal een belangrijke bijdrage leveren voor de keuzes die dienen te worden gemaakt, ook ten aanzien van de scope.

Alle geïnteresseerde partijen wordt gevraagd mee te werken aan het beantwoorden van de vragen van het NIPV en veiligheidsregio's.

Inhoud

1	Inleiding	4
1.1	Het NIPV en de veiligheidsregio's	4
1.2	Doel van de marktconsultatie	4
1.3	Huidige situatie / aanleiding	5
1.4	Gewenste situatie	6
2	Procedure marktconsultatie	7
2.1	Vorm	7
2.2	Voorbehoud	7
2.3	Contactpersoon	8
2.4	Planning	8
2.5	Stellen van vragen	8
2.6	Instructies voor beantwoording	8
3	Vragen	9

1 Inleiding

1.1 Het NIPV en de veiligheidsregio's

Nederland is verdeeld in 25 veiligheidsregio's (VR's). Iedere veiligheidsregio zet zich in voor de veiligheid van de inwoners en bezoekers van dat gebied. Zo zorgt de veiligheidsregio ervoor dat er een brandweer is. Ook maakt de veiligheidsregio afspraken over de aanpak van rampen en crises. Een goede samenwerking tussen hulpverleningsdiensten, overheden, bedrijven en burgers is daarbij belangrijk.

Het Nederlands Instituut Publieke Veiligheid (NIPV) is het publiek kennisinstituut dat veiligheidsregio's, Rijksoverheid en crisispartners onderling verbindt en versterkt met onderzoek, onderwijs, ondersteuning en informatie. Het NIPV fungeert als een 'centre of expertise' als het gaat om hoogwaardige kennis van crisisbeheersing en brandweezorg. Zo draagt het NIPV bij aan een veiliger en veerkrachtiger Nederland.

De wettelijke taken van een veiligheidsregio zijn onder meer (zie ook de Wet op de Veiligheidsregio's):

- > Opstellen van het risicoprofiel: inventarisatie van de kans op branden, rampen en crises;
- > Adviseren over het voorkomen van branden, rampen en crises, bijvoorbeeld aan bedrijven;
- > Organiseren van de rampenbestrijding en de crisisbeheersing;
- > Aanschaf en onderhoud van gemeenschappelijk materieel: brandweervoertuigen, redgereedschap, ambulances etc.;
- > Functioneren van de brandweer, de GHOR en de meldkamer;
- > Opstellen van het regionaal crisisplan; en
- > Inrichten en in stand houden van de informatievoorziening binnen de diensten van de Veiligheidsregio en andere relevante diensten en organisaties.

Ook de VR's en het NIPV moeten weerbaar zijn tegen cyberdreigingen. Het project 'Versnellingsplan Informatieveiligheid' is een project dat vanuit een opdracht van het Veiligheidsberaad inzet op het verbeteren van de informatieveiligheid van de VR's en het NIPV. De laatste jaren heeft de nadruk gelegen op de 'basis op orde' brengen door VR's en het NIPV te ondersteunen bij de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Nu verlegt het Versnellingsplan de aandacht naar o.a. monitorings- en responsdiensten.

1.2 Doel van de marktconsultatie

Dit document heeft als doel input op te halen ten behoeve van de eventuele toekomstige aanbesteding(en). Dit document tracht de daartoe benodigde informatie te verschaffen.

Met deze marktconsultatie wil het projectteam van het Versnellingsplan Informatieveiligheid, die als facilitator optreedt richting de VR's en het NIPV, een duidelijk beeld krijgen van wat de mogelijkheden en (eventuele) beperkingen zijn in relatie tot onze wensen, eisen en mogelijke aanbestedingsvormen.

In het bijzonder zijn we op zoek naar de volgende zaken:

- Inzicht te verkrijgen in de trends, ontwikkelingen, technische mogelijkheden en dienstverlening van leveranciers.
- Met de markt te kunnen spiegelen over kansen en mogelijkheden.
- Leveranciers stimuleren om ideeën en oplossingen in te brengen in het kader van de voorbereiding van de eventuele aanbesteding(en).
- Het kunnen bepalen van een aanbestedingsstrategie, mogelijke nadere planningen en objectieve gunningscriteria.

De uitkomsten van de marktconsultatie zullen worden gebruikt om te bepalen of de opdracht in de markt gezet gaat worden en voor het bepalen van de juiste aanbestedingsstrategie.

Het is niet de bedoeling dat op dit moment concrete aanbiedingen worden gedaan.

1.3 Huidige situatie / aanleiding

Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supply-chain, netwerken, systemen en (gevoelige) informatie.

Monitoring- en detectiediensten zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren.

Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan. Vervolgens kan op basis van deze alarmen opvolging gegeven worden om mitigerende maatregelen te nemen. Dit soort diensten brengen organisaties veelal samen onder de noemer: Managed Detection & Respons (MDR). De aanvullende diensten die hierbij aangeboden worden zijn onder andere de diensten vanuit een Security Operations Center (SOC).

Het project waar deze marktconsultatie deel van uitmaakt is een samenwerking van 10 VR's en het NIPV. Er is op basis van vrijwillige deelname gekeken welke VR's behoefte hebben om meer samen te werken op dit thema. Deze VR's en het NIPV nemen deel in dit project. Deelnemende VR's en het NIPV werken hierin samen om MDR en SOC-diensten te verwerven. Daarvoor is er aanvullend inzicht en kennis nodig die middels deze marktconsultatie getracht wordt op te halen. Het is niet gesteld dat dit een gezamenlijke aanbesteding moet zijn. Er wordt enerzijds onderzocht wat de uitvraag zou moeten zijn, anderzijds wordt uitgezocht hoe deze het beste in de markt gezet kan worden en of er in het aanbestedingstraject ook gezamenlijk wordt verworven of juist niet.

Hierbij willen we zowel rekening houden met de mogelijkheden die de markt biedt, maar ook met hoe de VR's in Nederland zijn georganiseerd. Deze marktconsultatie heeft o.a. tot doel om daar meer informatie over op te halen, zodat de uiteindelijke uitvraag zo goed mogelijk passend is bij de behoefte van de VR's en het NIPV als bij de mogelijkheden van de markt.

Sommige VR's hebben al bepaalde vormen van dienstverlening op dit gebied. Ook niet alle VR's zijn op dit moment aangesloten bij dit initiatief vanuit het Versnellingsplan Informatieveiligheid. Het is echter niet uit te sluiten dat dit op een ander moment wel zo gaat zijn. Op dit moment is dit initiatief vanuit het Versnellingsplan wel te typeren als het grootste onderlinge samenwerkingsverband binnen de sector op dit onderwerp.

1.4 Gewenste situatie

Het Versnellingsplan Informatieveiligheid beoogt met de voorgenomen opdracht het volgende te bereiken:

Het vergroten van de cyberweerbaarheid voor deelnemende VR's en het NIPV door het verwerven van externe MDR-diensten. Hieronder wordt het inrichten van een baseline verstaan op de gebieden:

- SOC-dienstverlening
- SIEM
- NDR
- EDR

Er wordt gestreefd naar implementatie van een minimale, door het Versnellingsplan samen met de deelnemers bepaalde, baseline met ruimte voor regionaal maatwerk (lees: aanvullingen op de baseline). Zie tevens het Programma van Eisen, bijlage 2.

De geschatte waarde van de opdracht is circa € 100.000,- à €150.000,- exclusief btw per deelnemer per jaar.

2 Procedure marktconsultatie

2.1 Vorm

Het NIPV faciliteert de marktconsultatie voor het Versnellingsplan. Het NIPV kiest ervoor om de marktconsultatie openbaar te publiceren op TenderNed en de marktpartijen in eerste instantie te vragen om hun antwoorden op de vragen schriftelijk in te dienen. Indien de gegeven antwoorden op de vragen uit de marktconsultatie een verduidelijking of toelichting behoeven, zullen daar waar nodig aanvullend nog mondelinge gesprekken ter toelichting op de gegeven antwoorden worden georganiseerd.

2.2 Voorbehoud

- Het NIPV vergoedt op geen enkele wijze kosten verbonden aan beantwoording van dit document of daaraan gerelateerde activiteiten. Het deelnemen aan de marktconsultatie is voor marktpartijen en het NIPV vrijblijvend.
- Partijen die deelnemen aan de marktconsultatie zullen bij de (Europese) aanbesteding(en) niet bevoor- of benadeeld worden. Alle partijen zullen over dezelfde informatie beschikken. Informatie die (commercieel) vertrouwelijk is, zal niet worden opgenomen in het verslag van de marktconsultatie en de aanbestedingsstukken.
- Van de marktconsultatie wordt een verslag gemaakt. Het verslag zal deel uitmaken van de documenten die ter beschikking worden gesteld tijdens de (Europese) aanbesteding met inachtneming van het vertrouwelijke karakter van concurrentiegevoelige informatie.
- Deze marktconsultatie dient uitdrukkelijk niet om een voorselectie te maken van marktpartijen in het kader van een mogelijke toekomstige aanbesteding. Evenmin vindt op enige wijze uitsluiting van bij de marktconsultatie betrokken partijen plaats in een mogelijke aanbesteding.
- Het NIPV houdt zich het recht voor om geen vervolg te geven aan deze marktconsultatie of afhankelijk van de uitkomst hiervan een bij de leveranciersmarkt passende verwervingsstrategie te kiezen.
- Er kunnen door marktpartijen geen rechten worden ontleend aan de ten behoeve van de marktconsultatie verstrekte informatie.
- De informatie die wordt verstrekt gedurende de marktconsultatie kan aanzienlijk afwijken van de informatie die in een later stadium wordt verstrekt ten aanzien van de aanbestedingsprocedure.
- De beantwoording van marktpartijen in deze marktconsultatie wordt eigendom van het NIPV. Het NIPV zal de verkregen informatie zorgvuldig behandelen en concurrentiegevoelige informatie vertrouwelijk behandelen.
- Het staat het NIPV vrij om de marktconsultatie – om welke reden dan ook – op ieder gewenst moment te beëindigen.
- Door deel te nemen aan de marktconsultatie geven partijen te kennen onvoorwaardelijk akkoord te zijn met deze bepalingen.
- De voertaal van deze marktconsultatie is Nederlands.

2.3 Contactpersoon

Naam: Nanet Kunst

Functie: Inkoopadviseur

Tijdens de marktconsultatie verloopt alle communicatie met het NIPV via bovenstaande contactpersoon. Indien er vragen of opmerkingen zijn over dit document, kunt u zich via de TenderNed-berichtenmodule richten tot de contactpersoon. Eventuele aanvullingen en correcties op de marktconsultaties zullen door het NIPV worden gepubliceerd op TenderNed.

2.4 Planning

Voor deze marktconsultatie heeft het NIPV de volgende planning beoogd:

	Actie	Datum
1.	Publicatie marktconsultatie op TenderNed	Maandag 3 maart 2025
2.	Uiterste datum en tijd voor het stellen van vragen over de marktconsultatie	Maandag 10 maart 2025, 17:00 uur
3.	Publicatie nota van inlichtingen	Vrijdag 14 maart 2025
4.	Uiterste datum en tijd voor het indienen van antwoorden door marktpartijen	Vrijdag 28 maart 2025
5.	Eventuele verdiepende (online) gesprekken	Dinsdag 8 april 2025

2.5 Stellen van vragen

Wanneer u vragen heeft over de gepubliceerde marktconsultatie, kunt u deze via de berichtenmodule van TenderNed aan het NIPV stellen, rekening houdend met de uiterste datum en tijd die hiervoor is opgenomen in de planning. Het NIPV zal de vragen verzamelen en geanonimiseerd beantwoorden in de nota van inlichtingen via TenderNed.

2.6 Instructies voor beantwoording

Omwille van een efficiënte tijdsbesteding bij zowel het NIPV als de geïnteresseerde marktpartijen verzoeken wij u de beantwoording in te vullen in het bijgevoegde Word document (Bijlage 1). U kunt dit document versturen via de berichtenmodule van TenderNed.

3 Vragen

De volgende vragen wensen de deelnemers graag schriftelijk beantwoord te krijgen. Het kan zijn dat een vraag voor u niet van toepassing is. In dat geval kunt u dat als antwoord aangeven.

Organisatie algemeen		
1.	Naam organisatie:	
2.	Naam en contactgegevens contactpersoon:	
3.	Wat is de grootte van uw organisatie, uitgedrukt in het aantal FTE dat u in dienst heeft?	
4.	Wat is globaal de jaarlijkse omzet van uw organisatie op de gezamenlijke onderdelen als genoemd in hoofdstuk 1.4 en wat is globaal uw marktaandeel?	
5.	Werkt u samen met andere bedrijven / onderaannemers in de keten bij dergelijke opdrachten? Zo ja, op welke aspecten?	

Organisatie - opdracht		
6.	Onze uitgangspunten op het gebied van dit project zijn verwoord in hoofdstuk 1. Op welke manier kunnen we volgens u dit doel het beste nastreven?	
7.	Welke producten c.q. diensten zijn volgens u in de markt beschikbaar in het kader van onze opdracht/behoefte?	
8.	Leg uit hoe onze behoefte op de gebieden van SOC-diensten, SIEM, NDR en EDR wel of niet samengaan in één uitvraag.	

9.	Hoe kunnen we onze wensen en eisen het beste kenbaar maken zodat dit een overzichtelijk geheel vormt? Welke filters c.q. onderwerpen stelt u hierbij voor?	
10.	Welke elementen zouden volgens u meer als 'eis' moeten worden weggezet en welke elementen meer als 'wens'?	
11.	De deelnemers zijn nog zoekende of deze uitvraag meer gezamenlijk of meer individueel in de markt gezet moet worden. Welke voor- en nadelen ziet u bij deze twee opties?	
12.	Welke doorlooptijd vindt u wenselijk om voldoende tijd te hebben voor implementatie, inleren en uitvoeren en waarom? Kunt u daarbij specificeren wat de gemiddelde doorlooptijd per fase is voor situaties gelijk aan die van ons?	
13.	Hoe stelt u voor dat we de door ons gestelde baseline in de uitvraag afzetten tegenover het, desnoods later, kunnen toevoegen van aanvullende opties door de contracthouders, zoals extra of een uitbreiding van diensten?	
14.	Wat is volgens u belangrijk bij het bepalen van een exit strategie? Wat is volgens u de beste manier om hier mee om te gaan?	

Concept programma van eisen (bijlage 2)		
15.	Kunt u op basis van het concept programma van eisen aangeven of: a. Er eisen gesteld worden die onnodig beperkend zijn? b. Er eisen gesteld worden die onnodig kostenverhogend zijn? c. Er eisen gesteld worden die onduidelijk zijn? d. Er eisen gesteld worden die om een andere reden niet wenselijk zijn? e. Er eisen gesteld worden die discriminerend zijn? f. Er eisen zijn die gemist worden? Indien ja, graag aangeven welke en waarom?	

Dienstverlening		
16.	Wat zijn volgens u de belangrijkste onderwerpen c.q. hoofdstukken die in een SLA terug zouden moeten komen en waarom?	
17.	Welke KPI's zijn volgens u hierbij belangrijk?	
18.	Wat zou volgens u moeten worden vastgelegd in een DAP op deze onderwerpen en waarom?	
19.	Kunt u uitleggen wat de (markt)definities zijn voor L1, L2 & L3 SOC-analisten?	
20.	Kunt u toelichten hoe dreigingsinformatie specifiek tot de VR's & NIPV worden vergaard en hoe deze binnen de context van de deelnemers wordt toegepast, en wat voor meerwaarde dit kan bieden voor de deelnemers?	
21.	Kunt u toelichten wat een gebruikelijke toepassing van	

	criticality niveau's zijn en de daarbij behorende Time To Respond?	
22.	Is het gebruikelijk dat een dienstverlener specifieke hard- en softwarecomponenten in abonnementsvorm levert die benodigd zijn voor het leveren van de dienstverlening? Zo ja, wat is hier gangbaar?	
23.	Kunt u uitleggen wat de voor- en nadelen zouden zijn als SOC, SIEM, NDR & EDR zowel los, als samen of een variant hierop kan worden afgenomen?	
24.	Kunt u toelichten welke architectuur vormen van uw dienstverlening mogelijk zijn of welke u absoluut niet ondersteunt. (Denk hierbij aan bijv. een (virtuele) appliance, aansluiten op een (on-premise) datalake, hybride construct etc..)	
25.	Kunt u toelichten welke industriestandaards er zijn m.b.t. use case frameworks en welke raadzaam zijn om te hanteren, en waarom?	
26.	Wat zijn volgens u relevante trainingen die door MSSP's kunnen worden gegeven die van toepassing zijn op de gevraagde dienstverlening? En waarom?	
27.	Waar houden volgens u de respons diensten op die nog te scharen zijn onder de MDR diensten, en waar gaat dit over in aanvullende respons diensten en hoe zien deze eruit? Denk hierbij aan escalatie naar CERT.	
28.	Kunt u toelichten hoeveel tijd u gemiddeld nodig heeft voor de afhandeling van diverse incidenten en welke impact op de kosten van de dienstverlening heeft het als dit door omstandigheden structureel meer blijkt te zijn.	

29.	Indien de CERT-dienstverlening niet vanuit uw organisatie wordt ingezet, hoe gaat u dan om met een samenwerking met een andere commerciële CERT-dienstverlener waar mogelijk al bestaande contractafspraken mee gemaakt zijn?	
30.	Sommige organisaties zullen veel taken uit een playbook zelf op kunnen pakken. Andere organisaties zullen meer acties bij de dienstverlener neerleggen. Wat is uw advies hoe om te gaan met dit verschil in uitvragen en welke impact heeft dit naar verwachting op de prijsstelling (en is die aanzienlijk of te verwaarlozen)?	

Prijsstelling algemeen		
31.	Welke informatie heeft u minimaal nodig om tot een juiste prijsstelling te komen?	
32.	Welke prijsmodellen zijn volgens u het meest praktisch bij het optioneel aanbieden van aanvullende respons diensten?	
33.	Kunt u een prijzenmodel aanleveren waarbij alle kosten van de dienstverlener zijn opgenomen, inclusief marktconforme tarieven voor de gevraagde diensten?	

Innovaties		
34.	Welke innovaties zijn recentelijk doorgevoerd in de door u aan te bevelen producten/diensten?	
35.	Welke innovaties zullen worden doorgevoerd gedurende de looptijd van de overeenkomst?	
36.	Welke kansen ziet u op het gebied van deze dienst in de komende vijf	

	jaar waar de deelnemers van kunnen profiteren?	
37.	Welke risico's ziet u op het gebied van deze dienst in de komende vijf jaar voor de deelnemers?	

Marktsituatie		
38.	Hoe zou u de huidige marktsituatie omschrijven? Ga in op het aantal aanbieders, de verhouding tussen de aanbieders op het gebied van marktaandeel, het lokale, regionale, nationale of internationale karakter van de markt en de ontwikkelingen op de markt in brede zin.	
39.	Op welke vlakken zit het onderscheidend vermogen van de markt met betrekking tot deze opdracht?	